Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Journal of Number Theory 109 (2004) 362–378

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Universal Kummer congruences mod prime powers

Arnold Adelberg*

Department of Mathematics, Grinnell College, Grinnell, IA 50112-0806, USA

Received 4 November 2003; revised 11 December 2003

Communicated by A. Granville

Available online 28 October 2004

Abstract

We have previously proved Kummer congruences mod primes p such that $p-1\nmid n$ for the universal divided Bernoulli numbers $\hat{B}_n/n$. In this paper we strengthen these congruences to hold mod powers of p.

MSC: Primary 11B68; 11B83; Secondary 11A07

Keywords: Universal Bernoulli numbers; Universal Kummer congruences

1. Introduction

The strongest form of the classical Kummer congruences says that if p is prime and $p-1\nmid m$ and $b_m=(1-p^{m-1})B_m/m$, where B_m is a Bernoulli number, then if ϕ is the Euler ϕ-function and $n\equiv m \bmod \phi(p^{N+1})$, then

$$b_n\equiv b_m \bmod p^{N+1}. \tag{1.1}$$

This periodic behavior of the divided Bernoulli numbers B_m/m is closely related to the existence of a p-adic zeta function (cf. [17]). The factor $1-p^{m-1}$ is called

* Corresponding author. Department of Mathematics and Computer Science, Grinnell College, Grinnell, IA 50112-0806, USA. Fax: +641 269 4984.

E-mail address: adelbe@math.grinnell.edu.

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.07.005

an *Euler factor*. The congruence is now usually proved by means of p-adic measures and p-adic integration (cf. [22]). As a corollary, we have a congruence without Euler factors, namely if $p-1 \nmid m$ and $n \equiv m \bmod \phi(p^{N+1})$ and $n, m \geqslant N+2$, then

$$B_n/n \equiv B_m/m \bmod p^{N+1}. \tag{1.2}$$

This congruence is the one that we generalize in this paper to the divided universal Bernoulli numbers $\hat{B}_n/n$. As our concluding examples in Section 4 show, the obvious strengthening to delta operators does not appear to work in the universal context. Our proofs, which imply the classical Kummer congruences as special cases, do not use p-adic measures or integration, but depend instead on use of many of the main results of elementary number theory, and in particular on careful p-adic analysis of factorials and of their congruences. The proofs are considerably more involved than our previous proofs of the $\bmod\, p$ universal Kummer congruences [1,2]. They are independent of those proofs, which are special cases, and use more refined analysis.

Definition 1.1. Let $c_1, c_2, \ldots$ be indeterminates over $\mathbf{Q}$ and let

$$F(t) = t + c_1 t^2/2 + c_2 t^3/3 + \cdots.$$

Let $G(t) = F^{-1}(t)$ be the compositional formal power series inverse of $F(t)$, i.e., $F\big(G(t)\big) = G\big(F(t)\big) = t$. The *universal Bernoulli numbers* $\hat{B}_n$ are defined by

$$t/G(t) = \sum_{n=0}^{\infty} \hat{B}_n t^n/n!. \tag{1.3}$$

It follows that $\hat{B}_n \in \mathbf{Q}[c_1, c_2, \ldots, c_n]$, and in fact $\hat{B}_n$ is a non-trivial $\mathbf{Q}$-linear combination of all the monomials of weight n, where c_i has weight i, so $\hat{B}_n$ is the sum of $p(n)$ monomials, where $p(n)$ is the partition function. We will use the explicit formula (3.1) for $\hat{B}_n/n$ in terms of the partitions of n throughout this paper.

If $c_1, c_2, \ldots$ are specialized to values in an extension K of $\mathbf{Q}$, then the $\hat{B}_n$ are also specialized to values in K, which we will continue to denote by $\hat{B}_n$, unless there is a chance of confusion. In particular if $c_i = (-1)^i$ then $F(t) = \log(1+t)$, so $G(t) = e^t - 1$, and $\hat{B}_n = B_n$. More generally if $c_i = a^i$ then $\hat{B}_n = (-a)^n B_n$. A variety of other specializations have also been investigated, particularly by algebraic topologists who work with the universal formal group and with complex cobordism rings (cf. [9,10]).

The *universal formal group* has formal group law $\tilde{F}(X, Y) = G\big(F(X) + F(Y)\big)$. In this context, F is called *formal group logarithm* and G is called the *formal group exponential*. The universal formal group is not defined over $\mathbf{Z}[c_1, c_2, \ldots]$, but is defined minimally over the *Lazard ring L*, which is the subring of $\mathbf{Q}[c_1, c_2, \ldots]$ generated by the coefficients of $\tilde{F}(X, Y)$. Clarke proved in [9] that $\hat{B}_n/n$ is p-integral if $p-1 \nmid n$, as part of his universal von Staudt Theorem. Miller [16] studied the specialization where c_i is the equivalence class of the complex projective space $\mathbf{C}P^i$, and proved that in that case L is the unitary bordism ring MU_*. He also proved that for this specialization, if k is odd and $k \neq 1$ then $\hat{B}_k/k \in L$.

The following theorem is essentially a restatement of the main result of this paper (Theorem 4.5).

Theorem. *Let $m \geqslant N+2$ and let $n = m + l(p-1)$ where $p^N | l$. Then*

(i) *if $m \not\equiv 0, 1 \bmod p-1$ then $\hat{B}_n/n \equiv c_{p-1}^l \hat{B}_m/m \bmod p^{N+1}\,\mathbf{Z}_p[c_1, \ldots, c_n]$.*
(ii) *If p is odd and $m = q(p-1)+1$ then*

$$\hat{B}_n/n \equiv c_{p-1}^l \hat{B}_m/m \;\; + c_{p-1}^{l+q-2}\Big(c_{p-1}c_1^p - c_{2p-1}\Big)l/2 \bmod p^{N+1}\mathbf{Z}_p[c_1, \ldots, c_n].$$

This theorem generalizes the mod p Kummer congruences which we previously proved for universal divided Bernoulli numbers in [1], since by [2, Remark 3.3], if p is an odd prime then

$$\hat{B}_p/p \equiv -c_p + (c_1 c_{p-1} + c_1^p)/2 \bmod p\,\mathbf{Z}_p[c_1, \ldots, c_p]. \tag{1.4}$$

It should be noted that unlike the classical Bernoulli numbers B_n where $B_n = 0$ if $n > 1$ and is odd, the universal Bernoulli numbers $\hat{B}_n \neq 0$ for all n. Case (i) contains non-trivial congruences where n and m are odd, but not when $m \equiv 1 \bmod p-1$, so is vacuous when $p = 3$. On the other hand, when $p \geqslant 3$ the congruences in case (ii) for n and m odd are all non-trivial. Observe that in case (ii) we have $l+q = (n-1)/(p-1)$.

An essential ingredient of our proof is a fundamental bound for the p-adic sizes of the coefficients of the terms in $\hat{B}_n/n$ (Proposition 3.2), which promises to be very helpful for congruences of universal Bernoulli numbers. This bound can be used to simplify Clarke's proof of the universal von Staudt Theorem in [9] as well as our proofs of the universal mod p Kummer congruences given in [1,2].

Carlitz [6,8] considered the question of Kummer congruences for specializations of the variables c_i. Snyder [20,21] considered this question in relation to formal groups and one-dimensional algebraic groups. His results show why the strongest form of the Kummer congruences does not hold in the universal case, since the universal formal group law is not defined over $\mathbf{Z}[c_1, c_2 \ldots]$ but only over L. The results of Carlitz and Snyder on Kummer congruences do not appear to apply directly to the divided universal Bernoulli numbers, and in particular the somewhat surprising significance of whether or not $m \equiv 1 \bmod p-1$ has apparently not been noticed before in the context of the universal Bernoulli numbers.

2. Number-theoretic preliminaries

Throughout this paper p will be an *odd prime*, which is implied by the generic hypothesis that $p-1 \nmid n$ throughout, except for the remarks after Corollary 3.3. We let

$v = v_p$ be the *standard p-adic valuation* of $\mathbf{Q}$, i.e., $v(r) = f$ if $p^f \parallel r$. We canonically extend v to $\mathbf{Q}[c_1, c_2, \ldots]$ by $v\big(\sum a_u c^u\big) = \min\{v(a_u)\}$ when $u = (u_1, \ldots, u_n) \in \mathbf{N}^n$ and $c^u = c_1^{u_1} \ldots c_n^{u_n}$.

We will freely use the following easily proven standard results (cf [18, Chapter 4]).

$$v\big((a+b)!\big) \geqslant v(a!) + v(b!), \tag{2.1}$$

$$v\big((lp)!\big) = l + v(l!), \tag{2.2}$$

$$v(a!) = v\big((\lfloor a/p \rfloor p)!\big) = \big(a - S(a)\big)/(p-1), \tag{2.3}$$

where S is the base p digit sum.

$$v(a!) \leqslant (a-1)/(p-1) \quad \text{if} \quad a > 0. \tag{2.4}$$

The following lemma is the odd prime case of [9, Proposition 2]. The basic proof technique, which also implies (2.2), is used in several of our proofs.

Lemma 2.1. *If p is an odd prime and $N = v(l)$ then*

$$(lp)!/(l!p^l) \equiv (-1)^l \bmod p^{N+1}.$$

Proof. Clearly

$$(lp)!/(l!p^l) = \prod_{\substack{i=1 \\ (i,p)=1}}^{lp} i. \tag{2.5}$$

If $l = \varepsilon p^N$ where $p \nmid \varepsilon$, then $(-1)^l = (-1)^\varepsilon$ since $p \neq 2$, so it will suffice to prove with $k = N + 1$ that

$$\prod_{\substack{i=1 \\ (i,p)=1}}^{p^k} i \equiv -1 \bmod p^k. \tag{2.6}$$

But this product is the product of all elements of the unit group $\mathbf{Z}_{p^k}^*$ which is known to be cyclic, so by the usual argument of pairing group elements with their inverses, the product is congruent to -1, which is the unique element of order 2. $\square$

Lemma 2.2. $v\big((\sum h_j p^j)!\big) \geqslant \sum(jh_j + v(h_j!))$.

Proof. By (2.1), it will suffice to show that $v\big((hp^\alpha)!\big) \geqslant \alpha h + v(h!)$, which we prove by induction on α. The result is trivial if $\alpha = 0$ and is true if $\alpha = 1$ by (2.2). Assume true for α where $\alpha \geqslant 1$. Then

$$v\big((hp^{\alpha+1})!\big) = hp^\alpha + v\big((hp^\alpha)!\big) \geqslant hp^\alpha + \alpha h + v(h!) \geqslant (\alpha+1)h + v(h!). \qquad \Box \tag{2.7}$$

Lemma 2.3. *If p is an odd prime and $0 < k \leqslant p$ then*

$$v(a!) \geqslant v(a+k)$$

unless $a = p - k$, in which case $v(a!) = v(a+k) - 1$.

Proof. We can assume $p \mid a+k$, i.e., $a + k = \varepsilon p^\alpha$ where $\alpha > 0$ and $p \nmid \varepsilon$. If $\varepsilon > 1$, then $a = \varepsilon p^\alpha - k \geqslant \varepsilon p^\alpha - p \geqslant (\varepsilon - 1)p^\alpha \geqslant p^\alpha$, so $v(a!) \geqslant v(p^\alpha) = \alpha$. Thus it suffices to assume $a + k = p^\alpha$ with $\alpha > 1$. Then $v(a!) = v\big((p^\alpha - p)!\big) \geqslant p^{\alpha-1} - 1 \geqslant \alpha$ since $\alpha \geqslant 2$ and $p \geqslant 3$. $\Box$

The following proposition, which is a big generalization of Wilson's Theorem, plays an important role in our proof of the universal Kummer congruences.

Proposition 2.4. *Let $v(l) = N$. Then*

(i) $\big((l+q)p\big)!/\big((l+q)!p^{l+q}\big) \equiv (-1)^l (qp)!/(q!p^q) \bmod p^{N+1}$.
(ii) $\big((l+q)p+a\big)!/\big((l+q)!p^{l+q}\big) \equiv (-1)^l (qp+a)!/(q!p^q) \bmod p^{N+1}$.
(iii) *If $a \geqslant ep$ then congruence* (ii) *holds* $\bmod\, p^{N+e}$.
(iv) *If $a \geqslant (e+1)p$ then*

$$\big((l+q)p+a\big)!/\big((l+q)!p^{l+q+e}\big) \equiv (-1)^l (qp+a)!/(q!p^{q+e}) \bmod p^{N+1}.$$

Proof. Note that Lemma (2.1) is the special case of (i) for $q = 0$. To prove (i), clearly

$$\big((l+q)p\big)! = \prod_{i=1}^{q}(lp+ip) \prod_{\substack{x=1 \\ (x,p)=1}}^{qp} (lp+x)(lp)! \tag{2.8}$$

Thus, using Lemma 2.1

$$\frac{\big((l+q)p\big)!}{(l+q)!p^{l+q}} = \prod_{\substack{x=1 \\ (x,p)=1}}^{qp} (lp+x)(lp)!/l!p^l \equiv \prod_{\substack{x=1 \\ (x,p)=1}}^{qp} x(-1)^l \bmod p^{N+1}. \tag{2.9}$$

Congruence (i) follows since

$$\prod_{\substack{x=1\\(x,p)=1}}^{qp} x = (qp)!/(q!p^q). \tag{2.10}$$

To deduce (ii), just multiply congruence (i) by

$$\prod_{x=1}^{a}\big((l+q)p+x\big) \equiv \prod_{x=1}^{a}(qp+x) \bmod p^{N+1}. \tag{2.11}$$

To deduce (iii), let $S=\{p,\ldots,ep\}$ and observe that

$$\begin{aligned}\prod_{x=1}^{a}\big((l+q)p+x\big) &= \prod_{i=1}^{e}(lp+qp+ip)\prod_{\substack{x=1\\x\notin S}}^{a}(lp+qp+x) \\ &= p^e\prod_{i=1}^{e}(l+q+i)\prod_{\substack{x=1\\x\notin S}}^{a}(lp+qp+x).\end{aligned} \tag{2.12}$$

Thus

$$\prod_{x=1}^{a}\big((l+q)p+x\big) \equiv p^e\prod_{i=1}^{e}(q+i)\prod_{\substack{x=1\\x\notin S}}^{a}(qp+x) \bmod p^{N+e}. \tag{2.13}$$

This concludes the deduction of (iii) from (i) since

$$\prod_{i=1}^{e}(qp+ip)\prod_{\substack{x=1\\x\notin S}}^{a}(qp+x) = \prod_{x=1}^{a}(qp+x). \tag{2.14}$$

Finally to deduce (iv), use congruence (iii) with e replaced by $e+1$, and then divide by p^e. $\square$

3. Explicit formulas and a critical bound for $\hat{B}_n/n$

If $u=(u_1,u_2,\ldots)\in\mathbf{N}^\infty$ with $u_i=0$ if $i\gg 0$ and $w(u)=\sum i\,u_i$, we identify u with a partition of $w(u)$, where u_i is the number of occurrences of the part i in the partition. If $d(u)=\sum u_i$, then $d(u)$ is the number of parts in the partition. We call $w(u)$ the *weight* of u and $d(u)$ the *degree* of u.

The key to our investigation is the following explicit formula, which comes from Lagrange inversion [2,9]

$$\frac{\hat{B}_n}{n}=\sum_{w=n}\tau_u c^u \tag{3.1}$$

where $u=(u_1,\ldots,u_n)\in\mathbf{N}^n$, $w=w(u)$, $d=d(u)$, $c^u=c_1^{u_1}\cdots c_n^{u_n}$, $\gamma_u=2^{u_1}\cdots(n+1)^{u_n}u_1!\cdots u_n!$, and

$$\tau_u=(-1)^{d-1}(n+d-2)!/\gamma_u. \tag{3.2}$$

The preceding notations will be used throughout the paper.

The following examples for small n illustrate the nature of the divided universal Bernoulli numbers. A more extensive list, for $1\leqslant n\leqslant 10$, can be found in the appendix to [9].

Example 3.1.

$$\begin{aligned}
\hat{B}_1&=c_1/2,\\
\hat{B}_2/2&=-c_1^2/4+c_2/3,\\
\hat{B}_3/3&=c_1^3/2-c_1c_2+c_3/2,\\
\hat{B}_4/4&=-15c_1^4/8+5c_1^2c_2-3c_1c_3-4c_2^2/3+6c_4/5.
\end{aligned}$$

Our plan is to prove the universal Kummer congruences (Theorem 4.5) as follows, with the notations of (3.1) and (3.2):

Let $n=m+l(p-1)$ and $p^N\mid l$. Suppose that $p-1\nmid n$ and $m\geqslant N+2$. We will show in Section 4 that if $u_{p-1}<l$, then except for certain cases that occur only if $n\equiv 1 \bmod p-1$, we have $v(\tau_u)\geqslant N+1$. We will also show that if $u_{p-1}\geqslant l$ and u' is defined by $u'_{p-1}=u_{p-1}-l$ and $u'_i=u_i$ if $i\neq p-1$, so that $d(u')=d(u)-l$, $w(u')=m$ and $c^u=c_{p-1}^l c^{u'}$, then $\tau_u\equiv\tau_{u'} \bmod p^{N+1}$. Combining these cases will prove the universal Kummer congruences Theorem 4.5(i) when $n\not\equiv 1 \bmod p-1$. Finally, analysis of the exceptional cases occurring when $n\equiv 1 \bmod p-1$ will prove Theorem 4.5(ii) to complete the demonstration of the theorem.

The following proposition gives a very useful bound for the p-adic size of the coefficient τ_u. It can be utilized to significantly simplify Clarke's proof of the universal von Staudt Theorem in [9] as well as the proof of the mod p Kummer congruences that we gave in [1,2]. Notations are as in formulas (3.1) and (3.2).

Proposition 3.2. *Let $w(u)=n$ and suppose that $p-1\nmid n$ and $u_{p-1}<\lfloor n/(p-1)\rfloor$.*

Let $e = v(\gamma_u) - v\big((pu_{p-1})!\big)$ *and* $n' = n - (p-1)u_{p-1}$. *Then*

$$n + d - 2 \geqslant (u_{p-1} + e + 1)p$$

except for the following cases where $(u_{p-1} + e + 1)p > n + d - 2 \geqslant (u_{p-1} + e)p$, *which occur when* $n = q(p-1) + 1$:

(i) $u_{p-1} = q - 1$, $u_1 = p = n'$ *and* $e = 1$;
(ii) $u_{p-1} = q - 1$, $u_p = 1$, $n' = p$ *and* $e = 0$;
(iii) $u_{p-1} = q - 2$, $u_{2p-1} = 1$, $n' = 2p - 1$ *and* $e = 1$.

Proof. Note that the hypotheses imply that $n \geqslant n' \geqslant p$. Let u' be the partition such that $u'_{p-1} = 0$ and $u'_i = u_i$ if $i \neq p - 1$. Then $w(u') = n'$ and $v(\gamma_{u'}) = e$. Also $n + d - 2 = pu_{p-1} + n' + d' - 2$, so replacing u by u', we can assume that $u_{p-1} = 0$.

Clearly we have $n + d = \sum(i+1)u_i$ and $e = \sum e_i$, where

$$e_i = v(i+1)u_i + v(u_i!), \tag{3.3}$$

so $e_i > 0$ only when $p \mid i + 1$ or $u_i \geqslant p$.

First consider the exceptional cases (i)–(iii): It is clear that $(i+1)u_i = (e_i + 1)p$ with $e_i = 1$ for cases (i) and (iii), where $i = 1$ and $u_i = p$, and $i = 2p - 1$ and $u_i = 1$ respectively, whereas $(i+1)u_i = (e_i + 1)p + 1$ with $e_i = 0$ for case (ii), where $i = p$ and $u_i = 1$.

We assert that

$$(i+1)u_i \geqslant (e_i + 1)p + 2 \tag{3.4}$$

for all other cases where $e_i > 0$ and $i \neq p - 1$, with the single exception that

$$(i+1)u_i = (e_i + 1)p \tag{3.5}$$

if $i = p^2 - 1$ and $p = 3$, with $u_i = 1$ and $e_i = 2$.

We must show that apart from this isolated exception and cases (i)–(iii) handled above,

$$(i+1)u_i \geqslant \big(v(i+1)u_i + v(u_i!) + 1\big)p + 2 \tag{3.6}$$

if $i \neq p - 1$ and $p \mid i + 1$ or $u_i \geqslant p$. Since the right-hand side of the inequality (3.6) involves only $v(i+1)$ rather than $i + 1$, it suffices to take $i + 1$ minimal for given $v(i+1)$, i.e., we have only to consider the cases $i = 1$ and $u_i \geqslant p$, $i = 2p - 1$ and $u_i \geqslant 1$, and $i = p^\alpha - 1$ with $\alpha \geqslant 2$ and $u_i \geqslant 1$. In all cases the inequality follows easily using the estimate (2.4) that $v(u_i!) \leqslant (u_i - 1)/(p-1) \leqslant (u_i - 1)/2$. The details follow:

First assume that $p \nmid i+1$ and $u_i \geqslant p$. If $i \geqslant 2$ and $u_i = p$, inequality (3.6) holds since $3p \geqslant 2p+2$. If $i=1$ and $p+1 \leqslant u_i < 2p$, then (3.6) holds since $2(p+1) = 2p+2$. Finally let $i=1$ and $u_i = kp+f$ where $k \geqslant 2$ and $0 \leqslant f < p$. Then it will suffice to prove that $2(kp) \geqslant \big(k+v(k!)+1\big)p+2$, which is true since $v(k!) \leqslant (k-1)/2$ so $k-1-v(k!) \geqslant 1$ if $k \geqslant 2$, and hence $p\big(k-1-v(k!)\big) \geqslant 2$. This concludes the case where $p \nmid i+1$.

Next assume that $\alpha = v(i+1) \geqslant 1$. If $\alpha = 1$ then (3.6) is equivalent to $kpu_i \geqslant \big(u_i+v(u_i!)+1\big)p+2$ if $k \geqslant 2$ and $u_i \geqslant 1$, except if $k=2$ and $u_i = 1$. But this inequality is equivalent to $p\big((k-1)u_i-1-v(u_i!)\big) \geqslant 2$, which is true since $v(u_i!) < (k-1)u_i - 1$ if $k \geqslant 2$ and $u_i \geqslant 1$ except if $k=2$ and $u_i=1$.

Finally assume that $\alpha \geqslant 2$. As previously noted, it suffices to take $i = p^{\alpha}-1$, and (3.6) is then equivalent to $p\big((p^{\alpha-1}-\alpha)u_i-1-v(u_i!)\big) \geqslant 2$, which is true if $\alpha \geqslant 2$ and $u_i \geqslant 1$ with the single exception $\alpha=2$, $p=3$ and $u_i=1$ since $p^{\alpha-1}-\alpha = 1$ if $p=3$ and $\alpha = 2$, and in all other cases $p^{\alpha-1}-\alpha > 1$, so $v(u_i!) < (p^{\alpha-1}-\alpha)u_i - 1$, and hence (3.6) holds as specified.

Finally if $u_i \geqslant 1$ then $(i+1)u_i \geqslant 2$, while if $(i+1)u_i \geqslant (e_i+1)p$ and $(j+1)u_j \geqslant (e_j+1)p$ then $(i+1)u_i + (j+1)u_j \geqslant (e_i+e_j+1)p + p \geqslant (e_i+e_j+1)p+2$. Since $p-1 \nmid n$, there exists $i \neq p^{\alpha}-1$ such that $u_i \geqslant 1$. If $e=0$ then as previously noted, since $n \geqslant p$, we have $n+d-2 \geqslant (e+1)p$, except if $n=p$ and $d=1$, which is case (ii). The desired inequality of the proposition for $n+d-2$ now follows by adding the "local" inequalities for each part i separately. $\square$

Corollary 3.3. *Suppose that* $p-1 \nmid n$ *and* $w(u) = n$ *and* $u_{p-1} < \lfloor n/(p-1) \rfloor$. *Then* $v(\tau_u) \geqslant 1$ *except for cases* (i)–(iii), *occurring when* $n \equiv 1 \bmod p-1$. *In these cases or if* $u_{p-1} \geqslant \lfloor n/(p-1) \rfloor$ *it is still true that* $v(\tau_u) \geqslant 0$.

Proof. With the same notations as before, if $n+d-2 \geqslant (u_{p-1}+e+1)p$ then $v\big((n+d-2)!\big) \geqslant v\Big(\big((u_{p-1}+e+1)p\big)!\Big) \geqslant v\big((pu_{p-1})!\big)+e+1$, so $v(\tau_u) \geqslant 1$. Explicit verification in cases (i)–(iii) where $n+d-2 \geqslant (u_{p-1}+e)p$ shows $v(\tau_u) \geqslant 0$, and that this is now the best bound.

Finally if $u_{p-1} \geqslant \lfloor n/(p-1) \rfloor$ then $n' < p-1$, so $e = v(\gamma_{u'}) = 0$ and $v(\tau_u) \geqslant 0$. $\square$

Remark 3.4. If we were to extend the preceding proposition to include the case where $p-1 \mid n$, in particular when $p=2$, we would get an alternative proof to Clarke's universal von Staudt Theorem. Since $v\big((pu_{p-1}-2)!\big) = v\big((pu_{p-1})!\big) - v(pu_{p-1})$, if $n = (p-1)u_{p-1}$ then $v(\tau_u) = -v(np)$. If $p=2$ and $u_{p-1} = 0$ then it is not hard to show that $v(\tau_u) \geqslant 0$ unless $n=3$ and $u_3 = 1$ or $n=6$ and $u_3=2$. By considering the congruences for τ_u in these cases, the full universal von Staudt Theorem [9, Theorem 5] would follow. If we could conveniently determine all u such that $v(\tau_u)=0$, we would have mod p Kummer congruences including the case where $p-1 \mid n$, which is not currently known.

4. The universal Kummer congruences

Definition 4.1. A partition u is called *reduced* if there is a part $g \in \mathbf{N}$ such that $u_g = 1$ and if $i \neq g$ and $u_i \neq 0$ then $i = p^\alpha - 1$.

The part g is needed to insure that $w(u) = n$, but is otherwise unimportant. It represents a kind of "garbage collection." Note that if u is reduced and $w(u) = n$ then $n \equiv g \bmod p - 1$, so if $p - 1 \nmid n$ then $p - 1 \nmid g$, and in particular $g \neq p^\alpha - 1$.

Lemma 4.2. *Assume $p - 1 \nmid m$ and let $n = (m + i)p - i = i(p - 1) + mp$ where $i \geqslant 0$. Let $w(u) = n$ and suppose that $d(u) \leqslant i + 1$. Then there exists a reduced u' such that $w(u') = n$, $d(u') \leqslant i + 1$ and $v(\tau_u) \geqslant v(\tau_{u'})$.*

Proof. We first construct a partition u'' such that if $u''_i \neq 0$ then $i = p^\alpha - 1$, with $w(u'') < n$:

(i) If $u_j \neq 0$ with $j = \varepsilon p^\alpha - 1$ and $p \nmid \varepsilon$ and $\varepsilon > 1$, let $u''_j = 0$ and $u''_k = u_k + u_j$ where $k = p^\alpha - 1$, i.e., transfer u_j to the part $p^\alpha - 1$.

(ii) If $u_j \geqslant p$ where $p \nmid j + 1$, let $u''_j = 0$ and $u''_{p-1} = u_{p-1} + \lceil u_j/(p - 1)\rceil - 1$, i.e., transfer to the part $p - 1$.

(iii) If $0 < u_j < p$ and $p \nmid j + 1$, let $u''_j = 0$, i.e., delete the part j from the partition. The partition u'' is formed by considering all parts, and should be thought of as loading the parts where $i = p^\alpha - 1$. All other parts of u where (i)–(iii) do not apply are unchanged. The partition u'' can be constructed from u one part at a time or all at once.

Observe that $v(\gamma_{u''}) \geqslant v(\gamma_u)$ by (2.1) and (2.4), and that $d(u'') = d(u)$ if all modifications are of type (i), while otherwise $d(u'') < d(u)$.

Next since $p - 1 \nmid n$, we have $g = n - w(u'') > 0$ and $g \neq p^\alpha - 1$. Let $u'_g = 1$ and $u'_j = u''_j$ if $j \neq g$. Then obviously u' is reduced and $w(u') = n$. Since $d' = d(u') = d(u'') + 1$, if $d(u'') < d(u)$ then $d(u') \leqslant d(u) \leqslant i + 1$. Hence $n + d - 2 \geqslant n + d' - 2$ and $v(\gamma_{u'}) = v(\gamma_{u''}) + v(g+1) \geqslant v(\gamma_u)$, so $v(\tau_u) \geqslant v(\tau_{u'})$ in this case. Finally assume $d(u'') = d(u)$. In this case all modifications are of type (i), so $n = \sum iu_i = \sum (k_j p - 1)h_j$. But $n = (m + i)p - i$, so $i \equiv \sum h_j = d(u) \bmod p$. Since $1 \leqslant d(u) \leqslant i + 1$, it follows that $d(u) = i$ and $d(u') = i + 1$. Also $n + d - 2 = \sum h_j k_j p - 2$, so $v\big((n + d - 2)!\big) = v\big((n + d' - 2)!\big)$ by (2.3). Since $v(\gamma_{u'}) \geqslant v(\gamma_{u''}) \geqslant v(\gamma_u)$, the proof is concluded. □

The following, rather delicate, lemma will give the mod p^{N+1} vanishing of the terms where $u_{p-1} < l$, which is an essential part of the Kummer congruences.

Lemma 4.3. *Let $n = (m + i)p - i$ with $p - 1 \nmid m$. Let u be reduced, with $w = n$ and $d \leqslant i + 1$. Then $v(\tau_u) \geqslant m - 1$.*

Proof. Let

$$h_j = u_k \quad \text{if} \quad k = p^j - 1 \tag{4.1}$$

with $j \geqslant 1$. Then $d = \sum h_j + 1$ and $n = \sum h_j(p^j - 1) + g$. Thus

$$n + d - 2 = \sum h_j p^j + g - 1. \tag{4.2}$$

Also

$$v(\gamma_u) = \sum \bigl(jh_j + v(h_j!)\bigr) + v(g+1). \tag{4.3}$$

Let

$$\delta = i + 1 - d = i - \sum h_j. \tag{4.4}$$

Then $\delta \geqslant 0$ since $d \leqslant i+1$ and

$$\delta + g = kp \tag{4.5}$$

where

$$k = m + i - \sum h_j p^{j-1}. \tag{4.6}$$

Since $g > 0$ and $\delta \geqslant 0$, we have $k > 0$, and if $\delta = 0$ then $g = kp$. On the other hand, $n = (m+i)p - i$ so

$$n + d - 2 = (m+i)p - (\delta + 1) = (m + i - k)p + g - 1. \tag{4.7}$$

Hence by (2.1), (2.2) and Lemma 2.2, we have

$$\begin{aligned} v\bigl((n+d-2)!\bigr) &\geqslant v\Bigl(\bigl((m+i-k)p\bigr)!\Bigr) + v\bigl((g-1)!\bigr) \\ &= m + i - k + v\bigl((\textstyle\sum h_j p^{j-1})!\bigr) + v\bigl((g-1)!\bigr) \\ &\geqslant m + i - k + \sum\bigl((j-1)h_j + v(h_j!)\bigr) + v\bigl((g-1)!\bigr). \end{aligned} \tag{4.8}$$

If

$$\Delta = \delta - k + 1 + v\bigl((g-1)!\bigr) - v(g+1) \tag{4.9}$$

then from (4.3), (4.8) and (4.9),

$$v(\tau_u) \geqslant m - 1 + \Delta. \tag{4.10}$$

Thus to complete the proof we must show that $\varDelta \geqslant 0$.

If $\delta - k \geqslant 0$, this is true by Lemma 2.3. Thus it will suffice to assume $\delta - k < 0$. In this case let

$$\delta = xp + r \quad \text{with} \quad 0 \leqslant r < p \tag{4.11}$$

so $x = \lfloor \delta/p \rfloor$. Clearly $x < \delta$ unless $\delta = 0 = r = x$, and $x < \delta - 1$ if $\delta \geqslant 2$ since $p \geqslant 3$.

Since $0 < g = kp - \delta = (k-x)p - r$, we have $k - x \geqslant 1$. But

$$g - 1 = (k-x)p - (r+1) = (k-x-1)p + (p-r-1) \tag{4.12}$$

so

$$v\big((g-1)!\big) = v\Big(\big((k-x-1)p\big)!\Big) = k - x - 1 + v\big((k-x-1)!\big). \tag{4.13}$$

Hence

$$\begin{aligned} \varDelta &= \delta - k + 1 + k - x - 1 + v\big((k-x-1)!\big) - v(g+1) \\ &= \delta - x + v\big((k-x-1)!\big) - v(g+1). \end{aligned} \tag{4.14}$$

Thus $\varDelta \geqslant 0$ unless $p \mid g+1$. Since $g + 1 = (k-x)p - (r-1)$, if $p \mid g+1$ then $r = 1$ and $g + 1 = (k-x)p$, so

$$\varDelta = \delta - x + v\big((k-x-1)!\big) - v(k-x) - 1. \tag{4.15}$$

Since $r \neq 0$, we have $\delta \neq 0$, so $\delta - x \geqslant 1$. It remains by Lemma (2.3) to show that $\delta - x = 1$ is impossible. If $\delta - x = 1$ then $\delta = 1$ and $x = 0$, and it will suffice to show that $k - x \neq p$. But if $k = p$ then $\delta + g = 1 + g = kp = p^2$, so $g = p^2 - 1$, which is impossible since $g \neq p^\alpha - 1$ as we have seen. $\square$

By combining the preceding lemmas we get

Corollary 4.4. *Let $n = (m+i)p - i$ with $p - 1 \nmid m$. Assume that $w = n$ and $d \leqslant i + 1$. Then $v(\tau_u) \geqslant m - 1$.*

We are now ready to turn to the universal Kummer congruences.

Theorem 4.5. *Let $n = m + l(p-1)$ and $p^N \mid l$. Suppose that $p - 1 \nmid m$ and $m \geqslant N + 2$.*

(i) *If $m \not\equiv 1 \bmod p - 1$ then $\hat{B}_n/n \equiv c_{p-1}^l \hat{B}_m/m \bmod p^{N+1}\,\mathbf{Z}_p[c_1, \ldots, c_n]$.*

(ii) *If* $m = q(p-1)+1$ *then*

$$\hat{B}_n/n \equiv c_{p-1}^l \hat{B}_m/m + c_{p-1}^{l+q-2}\left(c_{p-1}c_1^p - c_{2p-1}\right)l/2 \bmod p^{N+1}\,\mathbf{Z}_p[c_1,\ldots,c_n].$$

Proof. First consider the terms $\tau_u c^u$ of $\hat{B}_n/n$ where $u_{p-1} \geqslant l$. First subtract l from u_{p-1}, i.e., $u'_{p-1} = u_{p-1} - l = q$ and $u'_i = u_i$ if $i \neq p-1$, so $w(u') = m$. Next subtract q from u'_{p-1}, i.e., $\dot{u}_{p-1} = 0 = u'_{p-1} - q$ and $\dot{u}_i = u_i$ if $i \neq p-1$.

Let $v(\gamma_{\dot{u}}) = e$, so $\gamma_{\dot{u}} = \varepsilon p^e$ where $p \nmid \varepsilon$. Since $d' = d(u') = d(u) - l$ and $\dot{d} = d(\dot{u}) = d' - q$, we have

$$n + d - 2 = lp + m + d' - 2 = lp + qp + \dot{n} + \dot{d} - 2. \tag{4.16}$$

Now use Propositions 2.4 and 3.2 with $a = \dot{n} + \dot{d} - 2$, noting that $\gamma_u = (l+q)!p^{l+q}\gamma_{\dot{u}}$ and $\gamma_{u'} = q!p^q\gamma_{\dot{u}}$. Then

$$\tau_u \equiv \tau_{u'} \bmod p^{N+1} \tag{4.17}$$

except for cases (i) and (iii) where $e = 1$ and $\dot{n} = p$ and $2p-1$ respectively: If $e = 0$, this follows from Proposition 2.4(ii), while if $a \geqslant (e+1)p$ we use Proposition 2.4(iv). If $e \neq 0$ then clearly $u_{p-1} < \lfloor n/(p-1) \rfloor$ so that $a \geqslant (e+1)p$ by Proposition 3.2, with the exception of cases (i) and (iii), which occur when $n \equiv 1 \bmod p-1$. Note that the q defined earlier in this proof conforms with the usage in Proposition 2.4, but is not exactly the same as the q in Proposition 3.2 or the q in Theorem 4.5(ii). We will resolve this notational inconsistency below when we return to the notation of Theorem 4.5(ii) to explicitly consider the two exceptional cases where $e > 0$ and $a < (e+1)p$.

Thus

$$\sum_{w=n}{}' \tau_u c^u \equiv c_{p-1}^l \sum_{w=m}{}'' \tau_u c^u \bmod p^{N+1}\,\mathbf{Z}_p[c_1,\ldots,c_n], \tag{4.18}$$

where $\sum'$ is summed over all u of weight n with $u_{p-1} \geqslant l$, with the exception of the two terms indicated above for cases (i) and (iii) for n if $n \equiv 1 \bmod (p-1)$, and $\sum''$ is summed over the corresponding non-exceptional terms of weight m.

We now turn to the two exceptional terms, which occur if and only if $m \equiv 1 \bmod (p-1)$.

If $m = q(p-1)+1$ and $u'_{p-1} = q-1$ and $u_1 = p$, then we assert that

$$\tau_u \equiv \tau_{u'} + l/2 \bmod p^{N+1}. \tag{4.19}$$

This is true since $u_{p-1} = l + q - 1$, so $d = l + q - 1 + p$ and

$$\begin{aligned}\tau_u &= (-1)^{d-1} \frac{(n+d-2)!}{(l+q-1)!p^{l+q-1}p!2^p} \\ &= (-1)^l(-1)^{q-1} \frac{\big((l+q)p+p-2\big)!(l+q)}{(l+q)!p^{l+q}(p-1)!2^p}.\end{aligned} \tag{4.20}$$

By Proposition 2.4(ii),

$$(-1)^l(-1)^{q-1} \frac{\big((l+q)p+p-2)!q}{(l+q)!p^{l+q}(p-1)!2^p} \equiv (-1)^{q-1} \frac{(qp+p-2)!q}{q!p^q(p-1)!2^p} \bmod p^{N+1}.$$

The right-hand side is the term $\tau_{u'}$. On the other hand

$$(-1)^l(-1)^{q-1} \frac{\big((l+q)p+p-2\big)!l}{(l+q)!p^{l+q}(p-1)!2^p} \equiv \frac{l}{2} \bmod p^{N+1}$$

by Fermat's Little Theorem, Wilson's Theorem, and Lemma 2.1 taken mod p.

Finally if $m = q(p-1)+1$, $u'_{p-1} = q-2$ and $u_{2p-1} = 1$ then

$$\tau_u \equiv \tau_{u'} - l/2 \bmod p^{N+1}, \tag{4.21}$$

since now we have $u_{p-1} = l + q - 2$, so $d = l + q - 1$ and

$$\begin{aligned}\tau_u &= (-1)^{l+q} \frac{\big((l+q-1)p+p-2\big)!}{(l+q-2)!p^{l+q-2}2p} \\ &= (-1)^{l+q} \frac{\big((l+q-1)p+p-2\big)!(l+q-1)}{(l+q-1)!p^{l+q-1}2}.\end{aligned} \tag{4.22}$$

By Proposition 2.4(ii) with q replaced by $q-1$,

$$\begin{aligned}&(-1)^l(-1)^q \frac{\big((l+q-1)p+p-2\big)!(q-1)}{(l+q-1)!p^{l+q-1}2} \\ &\quad\equiv (-1)^q \frac{\big((q-1)p+p-2\big)!(q-1)}{(q-1)!p^{q-1}2} \bmod p^{N+1}.\end{aligned}$$

The right-hand side is the term $\tau_{u'}$. On the other hand

$$(-1)^{l+q} \frac{\big((l+q-1)p+p-2\big)!\,l}{(l+q-1)!p^{l+q-1}2} \equiv -\frac{l}{2} \bmod p^{N+1}$$

by Wilson's Theorem and the mod p special case of Lemma 2.1.

We now turn our attention to the terms where $u_{p-1} < l$. To finish the proof, it will suffice to show that if $w(u) = n$ and $u_{p-1} < l$ then $\tau_u \equiv 0 \bmod p^{N+1}$ if $m > N+1$, with the single exception where u is given by $u_{p-1} = l-1$ and $u_{2p-1} = 1$. In this case, the argument just given shows $\tau_u \equiv -l/2 \bmod p^{N+1}$, which is consistent with our Kummer congruences when $q = 1$ and $m = p$.

Assume henceforth that $u_{p-1} = l - x$ with $x \geqslant 1$. First assume that $n+d-2 \geqslant lp$, so we can consider $n+d-2 \geqslant (l+k)p$ with k maximal. Then with our usual notation, $\dot{n} = n - (l-x)(p-1) = m + x(p-1)$. Thus since $\dot{n} > m$, the only exceptional case of Proposition 3.2 that can occur is when $m = p$, $x = 1$ and $\dot{n} = 2p-1$, which was previously considered. Thus if $e = v(\gamma_{\dot{u}})$ then by Proposition 3.2

$$n + d - 2 \geqslant (l - x + e + 1)p. \tag{4.23}$$

On the other hand, $n + d - 2 \geqslant (l+k)p$ so

$$\begin{aligned} v\Big((n+d-2)!/\big((l-x)p\big)!\Big) &\geqslant v\Big(\big((l+k)p\big)!/\big((l-x)p\big)!\Big) \\ &\geqslant k + v(lp) + x - 1 \end{aligned} \tag{4.24}$$

so if $v(\tau_u) < v(lp)$ then $e > k + x - 1$, i.e., $e \geqslant k + x$. But then by (4.23)

$$n + d - 2 \geqslant (l + k + 1)p \tag{4.25}$$

which contradicts the assumed maximality of k.

Thus we are reduced to the case where $u_{p-1} = l - x$ with $x > 0$ and $n+d-2 < lp$, i.e., $m + l(p-1) + d < lp + 2$, or $m + d \leqslant l + 1$. Since $p - 1 \nmid n$, we have $u_{p-1} = l - x < d \leqslant l + 1 - m$, so $x \geqslant m$. Thus $x = m + i$ with $i \geqslant 0$. Then

$$w(\dot{u}) = m + x(p-1) = (m+i)p - i \tag{4.26}$$

and

$$d(\dot{u}) = d - (l - x) \leqslant x + 1 - m = i + 1. \tag{4.27}$$

But $u_{p-1} = l - x$, so $n + d - 2 \geqslant (l-x)p + \dot{n} + \dot{d} - 2$ and $v(\tau_u) \geqslant v(\tau_{\dot{u}})$ by (2.1) and (2.2). Since $m - 1 \geqslant v(lp)$ by assumption and we can replace n and u by $\dot{n} = (m+i)p - i$ and $\dot{u}$, respectively, Corollary 4.4 gives $\tau_u \equiv 0 \bmod p^{N+1}$.

Hence by (4.18), (4.19), and (4.21), the proof is complete. $\square$

Taking into account the single exception considered in the previous proof where $m = p$, and $u_{p-1} = l - 1$ and $u_{2p-1} = 1$, we have the following corollary.

Corollary 4.6. *Suppose that $p-1 \nmid n$ and $n-l(p-1) > N+1$, where $p^N \mid l$. Then*

$$\hat{B}_n/n \equiv 0 \bmod \left(p^{N+1},\ c_{p-1}^l\right) \mathbf{Z}_p[c_1, \dots c_n]$$

unless $n = l(p-1)+p$, in which case

$$\hat{B}_n/n \equiv -c_{p-1}^{l-1} c_{2p-1}\, l/2 \bmod \left(p^{N+1},\ c_{p-1}^l\right) \mathbf{Z}_p[c_1, \dots, c_n].$$

Finally, we give some examples to show there are no obvious improvements to our universal Kummer congruences.

Example 4.7. It does not appear to be possible to weaken the hypothesis $m \geqslant N+2$ in Theorem 4.5 by incorporating an appropriate "Euler factor" for the universal Bernoulli numbers. As an example, if $n = 22$, $m = 2$, $l = 5$, and $p = 5$ so that $N = v(l) = 1$, the two partitions u of n where $u_4 = 3$, $u_{10} = 1$ and where $u_4 = 1$, $u_9 = 2$ both satisfy $1 = v(\tau_u) < N+1 = 2$, so these terms, which do not correspond to terms for m since $u_{p-1} < l$, will occur non-trivially in any Kummer congruence mod p^{N+1}, and no "Euler factor" will ameliorate the situation.

Example 4.8. If Δ increments indices by $p-1$, i.e.,

$$\Delta(B_m/m) = B_{m+p-1}/(m+p-1) - B_m/m,$$

then it is known that (cf. [7])

$$\Delta^r(B_m/m) \equiv 0 \bmod p^r \text{ if } m \geqslant r+1 \text{ and } p-1 \nmid m. \tag{4.28}$$

If we make the obvious modification

$$\Delta(\hat{B}_m/m) = \hat{B}_{m+p-1}/(m+p-1) - c_{p-1}\hat{B}_m/m, \tag{4.29}$$

then the congruence $\Delta^r(\hat{B}_m/m) \equiv 0 \bmod p^r \mathbf{Z}[c_1, c_2, \dots]$ is not always true if $m \geqslant r+1$, even if $m \not\equiv 0, 1 \bmod p-1$. As an example, related to the Euler factor issue, if $n = 11$, $m = 3$, $p = 5$ and $r = 2$, the partition u where $u_9 = u_2 = 1$ has $v(\tau_u) = 1 < r$, so the term appears non-trivially in the congruence mod $p^r \mathbf{Z}_p[c_1, c_2, \dots]$ since $u_{p-1} = 0$. The congruence even fails in certain instances where $u_{p-1} \geqslant r$, e.g., let $n = 31$, $m = 7$, $p = 5$ and $r = 6$. Then if $u_4 = 7$ and $u_2 = u_5 = 1$, the coefficient of $c^u \bmod p^r$ in $\Delta^r(\hat{B}_m/m)$ is non-zero, namely its p-adic valuation is $r-1$. Empirical evidence suggests that for the monomials c^u where $u_{p-1} \geqslant r$, the congruence for $\Delta^r(\hat{B}_m/m)$ may hold mod $p^{r-1}\mathbf{Z}_p[c_1, c_2, \dots]$ in general, and may hold mod $p^r \mathbf{Z}_p[c_1, c_2, \dots]$ if $p > r$.

References

[1] A. Adelberg, Kummer congruences for universal Bernoulli numbers and related congruences for poly-Bernoulli numbers, Int. Math. J. 1 (1) (2002) 119–135 MR 2002d: 11023.

[2] A. Adelberg, Universal higher order Bernoulli numbers and Kummer and related congruences, J. Number Theory 84 (1) (2000) 119–135 MR 2001g: 11018.

[3] A. Adelberg, Congruences of p-adic integer order Bernoulli numbers, J. Number Theory 59 (2) (1996) 374–388 MR 97e: 11028.

[4] A.J. Baker, F. Clarke, N. Ray, L. Schwartz, On the Kummer congruences and the stable homotopy of BU, Trans. Amer. Math. Soc. 316 (1989) 385–432 MR 90c: 55003.

[5] J. Bernoulli, Ars Conjectandi, Basel, 1713.

[6] L. Carlitz, Criteria for Kummer's congruences, Acta Arith. 6 (1961) 375–391 MR 27: 4786.

[7] L. Carlitz, Some theorems on Kummer's congruences, Duke Math. J. 19 (1952) 423–431 MR 15: 10f.

[8] L. Carlitz, Some properties of Hurwitz series, Duke Math. J. 16 (2) (1949) 285–295 MR 10: 593e.

[9] F. Clarke, The universal von Staudt theorems, Trans. Amer. Math. Soc. 315 (1989) 591–603 MR 90a: 11026.

[10] I. Dibag, An analogue of the von Staudt–Clausen theorem, J. Algebra 87 (1984) 332–341 MR 85j: 11028.

[11] F.T. Howard, Congruences and recurrences for Bernoulli numbers of higher order, Fibonacci Quart. 32 (1994) 316–328 MR 95k: 11021.

[12] W. Johnson, p-adic proofs of congruences for the Bernoulli numbers, J. Number Theory 7 (1975) 251–265 MR 51: 12687.

[13] N.M. Katz, The congruences of Clausen–von Staudt and Kummer for Bernoulli–Hurwitz numbers, Math. Ann. 216 (1975) 1–4 MR 52: 8136.

[14] E.E. Kummer, Über eine allgemeine Eigenschaft der rationalen Entwicklungscoefficienten eines bestimmten Gattung analytischer Funktionen, J. Reine Angew. Math. 41 (1851) 368–372.

[15] A.T. Lundell, On the denominator of generalized Bernoulli numbers, J. Number Theory 26 (1987) 79–88 MR 88d: 11020.

[16] H. Miller, Universal Bernoulli numbers and the S^1-transfer, Current Trends in Algebraic Topology, part 2 (London, Ont. 1981), Canad. Math. Soc. Conf. Proc., vol. 2, American Mathematical Society, Providence, RI, 1982, pp. 437–449, MR 85b: 55029.

[17] M. Ram Murty, Introduction to p-adic analytic number theory, AMSCIP Studies in Advanced Mathematics, vol. 27, American Mathematical Society, Providence, RI, 2002, MR 2003c: 11108.

[18] I. Niven, H. Zuckerman, H. Montgomery, An Introduction to the Theory of Numbers, 5th ed., Wiley, New York, 1991 MR 91i: 11001.

[19] N. Ray, Extensions of umbral calculus: penumbral coalgebras and generalized Bernoulli numbers, Adv. Math. 61 (1986) 41–100 MR 88b: 0519.

[20] C. Snyder, Kummer congruences for the coefficients of Hurwitz series, Acta Arith. 40 (1982) 175–191 MR 83d: 10016.

[21] C. Snyder, Kummer congruences in formal groups and algebraic groups of dimension one, Rocky Mountain J. Math. 15 (1985) 1–11 MR 86j: 14044.

[22] P.T. Young, Congruences for Bernoulli Euler and Stirling numbers, J. Number Theory 78 (1999) 204–227 MR 2000i: 11038.

[23] P.T. Young, Kummer congruences for values of Bernoulli and Euler polynomials, Acta Arith. 99 (3) (2001) 277–288 MR 2002g: 11-21.